

## ABSTRACT

Method and apparatus for secure transmissions. Each user is provided a registration key. A long-time updated broadcast key is encrypted using the registration key and provided periodically to a user. A short-time updated key is encrypted using the broadcast key. The short-time key is available with each broadcast message, wherein sufficient information to calculate the short-time key is provided in an Internet protocol header preceding the broadcast content. Broadcasts are then encrypted using the short-time key, wherein the user decrypts the broadcast message using the short-time key.